TrackHackMe Room :-Hello World

1. **Link:-**https://tryhackme.com/room/hello

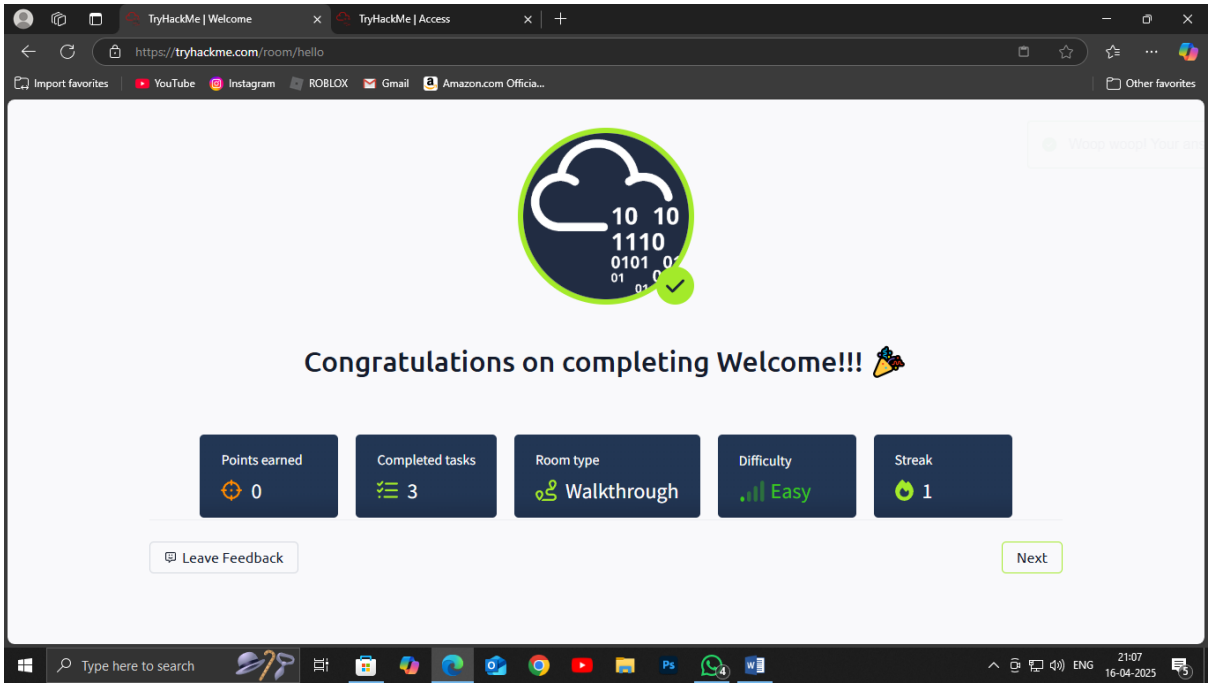
2. **Learning Objective:-**Understand how TryHackMe rooms work, interact with the THM interface, and learn the basic structure of cybersecurity training rooms. This room is designed for absolute beginners.

3. **Key Tools/Commands Used:-**
   - THM Web Interface
   - No command-line tools required
   - Navigation via browser
   - Answering questions in the THM interface

4. **Concepts learned:-**
   - Basic navigation of TryHackMe rooms
   - Understanding task-based learning structure
   - Submitting answers to questions
   - Importance of reading instructions carefully
   - Initial exposure to cybersecurity learning platforms

5. **Walkthrough / How You Solved It:-**
   - **Started the Room:** Clicked on the "Join Room" button.
   - **Read through the Introduction:** Each task had a short description. Carefully read the information provided.
   - **Answered Questions:**
     - **1.**Most were straightforward and required close reading of the provided text.
     - **2.**Questions included identifying keywords or values from the text.
   - **Followed Instructions:** Some tasks required clicking or exploring parts of the interface (like starting a machine or clicking a link).
   - **Completed the Room:** Answered all the questions to 100%

6. **Reflections or Notes:-**
   - A great introduction to the TryHackMe platform, especially for those new to cybersecurity or online labs.
   - Reinforced the importance of attention to detail, as many questions tested comprehension.
   - No prior technical knowledge was needed — perfect for total beginners.
   - Sets the tone for more complex rooms by introducing how tasks and questions are structured.



TrackHackMe Room :- How to Use TryHackMe

1. **Link:-**https://tryhackme.com/room/howtousetryhackme
2. **Learning Objective:-**Learn how to interact with TryHackMe labs, including deploying machines, using the in-browser attack box, understanding the layout of rooms, and getting comfortable with the environment before jumping into technical content.

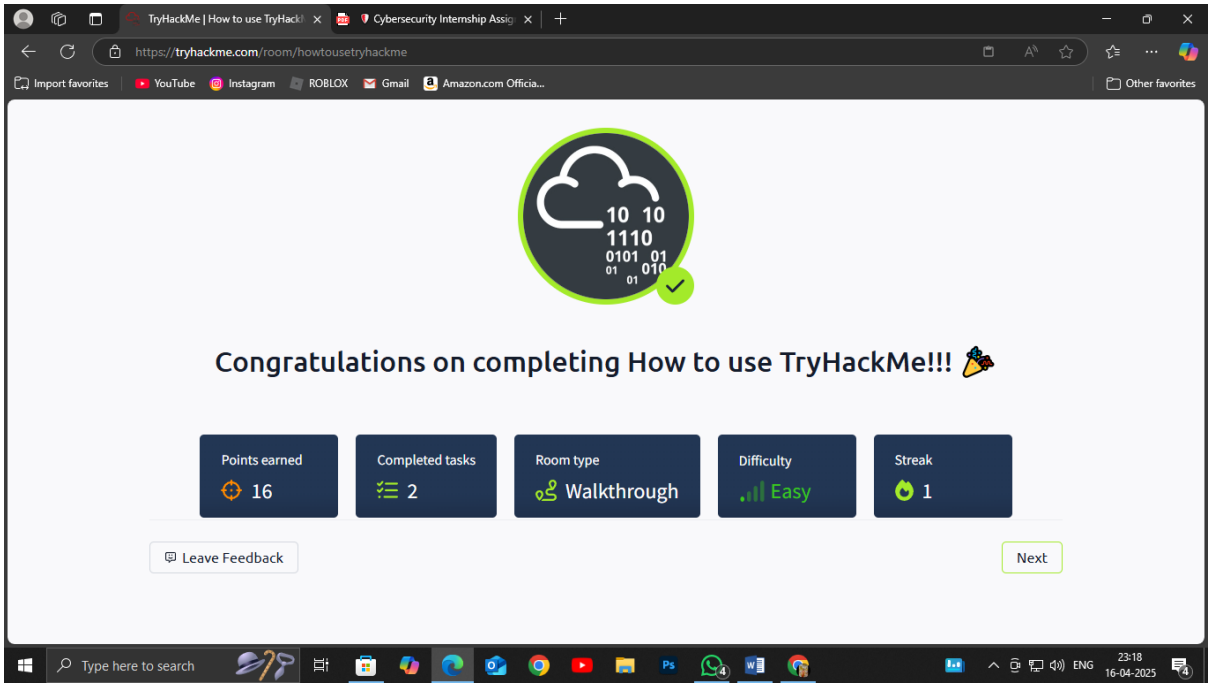
3. **Key Tools/Commands Used:-**
   - TryHackMe AttackBox
   - Web browser (interface navigation)
   - No terminal commands needed — interaction was mostly UI-based
   - Machine Deployment Button
   - Split-screen interface between VM and browser

4. **Concepts learned:-**
   - How to **deploy and interact with virtual machines** in TryHackMe
   - Difference between **browser-based AttackBox** and connecting via **VPN**
   - Overview of **room/task/question** structure
   - Navigating rooms, understanding how hints and questions are presented
   - Importance of **terminating** machines after completion

5. **Walkthrough / How You Solved It:-**
   - Joined the Room: Clicked “Join Room” and started with the first task.
   - Read Through the Introductory Tasks: The room gives a breakdown of what a TryHackMe room contains and how it's structured.
   - Deployed the Machine: Followed the instructions to deploy a target machine and waited for it to boot.

- Launched the AttackBox: Opened the in-browser AttackBox to interact with the target (though interaction was minimal in this room).
- Answered Questions: These were based on reading the room content carefully and clicking on or interacting with the interface.
- Completed All Tasks: Followed the tasks sequentially and answered each question until the room showed 100% completion.

6. **Reflections or Notes:-**
   - This room is essential for first-time users of TryHackMe.
   - No technical knowledge is needed — it's focused on platform orientation.
   - It clearly explains the difference between using the AttackBox vs. connecting your own Kali VM.
   - Reinforces the habit of always terminating machines to avoid usage limits.
   - Great prep before diving into hands-on hacking or networking rooms.



TrackHackMe Room :- Getting Started

1. **Link:-** [TryHackMe | Getting Started]
2. **Learning Objective:-**Introduce users to the core concepts of cybersecurity, virtual machines, AttackBox usage, and TryHackMe's room/task/question flow — while completing a simple, interactive challenge to apply what was learned.

3. **Key Tools/Commands Used:-**
   - TryHackMe AttackBox
   - In-browser terminal
   - Web-based VM interaction
   - Basic Linux commands (e.g., ls, cd, cat)
   - Web browser navigation

4. **Concepts learned:-**

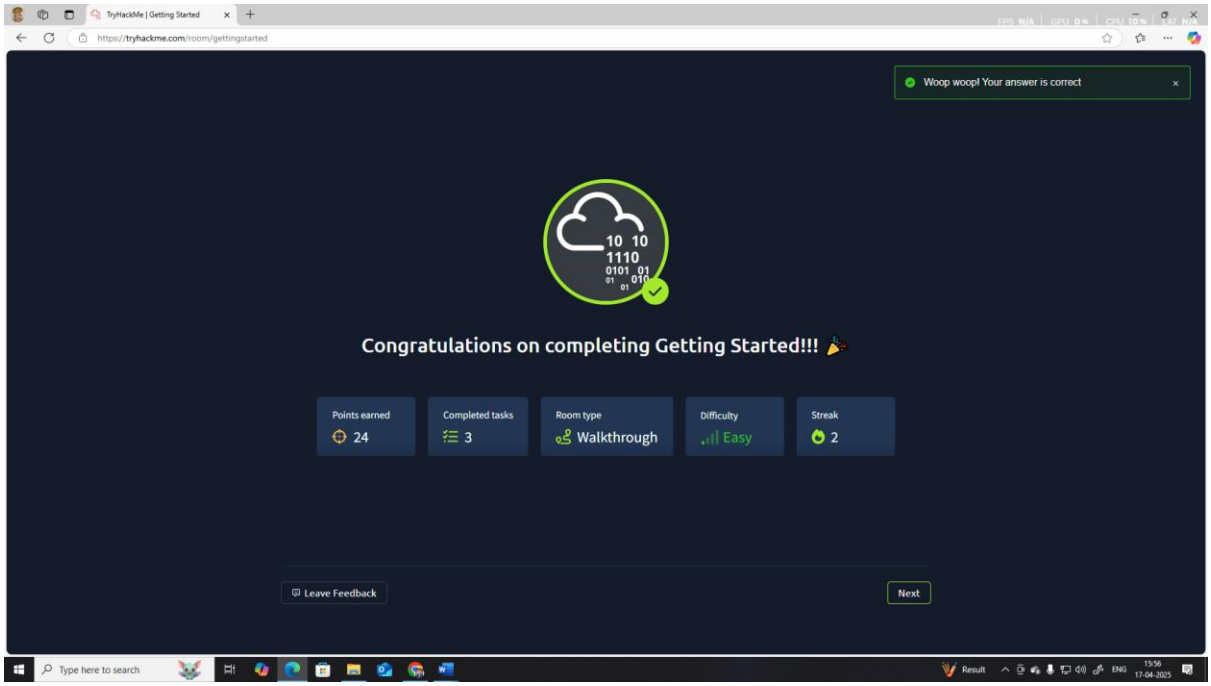
- How to navigate a TryHackMe room and complete tasks
- Basics of interacting with a virtual machine in the browser
- How to use terminal commands in a real-world hacking lab environment
- Importance of exploring file systems and reading files
- Introduction to CTF-style (Capture the Flag) tasks — finding and submitting flags

5. **Walkthrough / How You Solved It:-**

- Joined the Room: Hit “Join Room” and started the first task.
- Deployed the Virtual Machine: Followed instructions to deploy the target system.
- Used the AttackBox: Opened the AttackBox to interact with the target machine through the browser.
- Followed Linux Command Instructions:
  - Ran basic commands like ls to list files and cd to change directories
  - Used cat <filename> to read the contents of specific files, which often contained flags.
- Answered Questions:
- Most questions were solved by reading the content of specific files or understanding the output of terminal commands.
- Captured and Submitted Flags: The room walked through how to identify and submit your first few flags (e.g., THM{example_flag}).
- Completed All Tasks: Progressed through all sections and received the green 100% completion badge.

6. Reflections or Notes:-

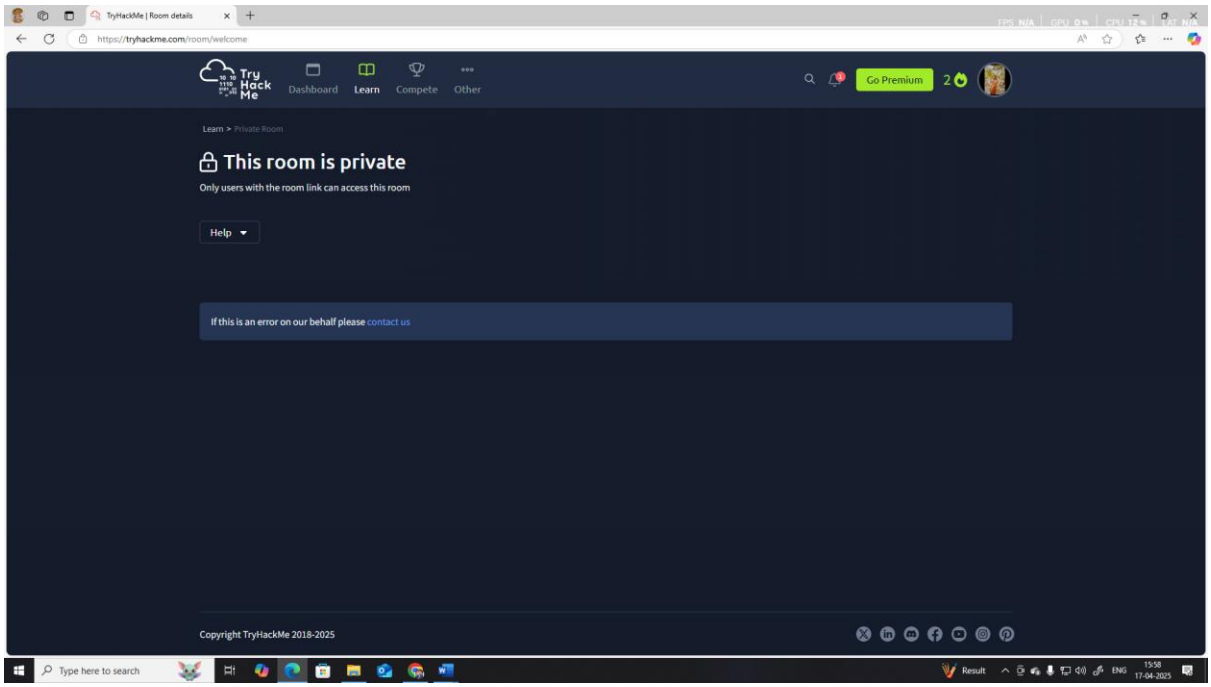
- Perfect introductory room for beginners with zero terminal experience.
- Reinforces how to navigate both the platform and a Linux environment.
- Encourages exploration and builds comfort with command-line interfaces.
- Great stepping stone to more advanced rooms like “Linux Fundamentals” or “Intro to Cyber Security.”
- Tip: If you're new to Linux, keep a cheat sheet handy — it'll help big time.



TrackHackMe Room :- Welcome

1 .**Link**:-[TryHackMe | Room details]

This room was private so I cant explore ṭhis room.



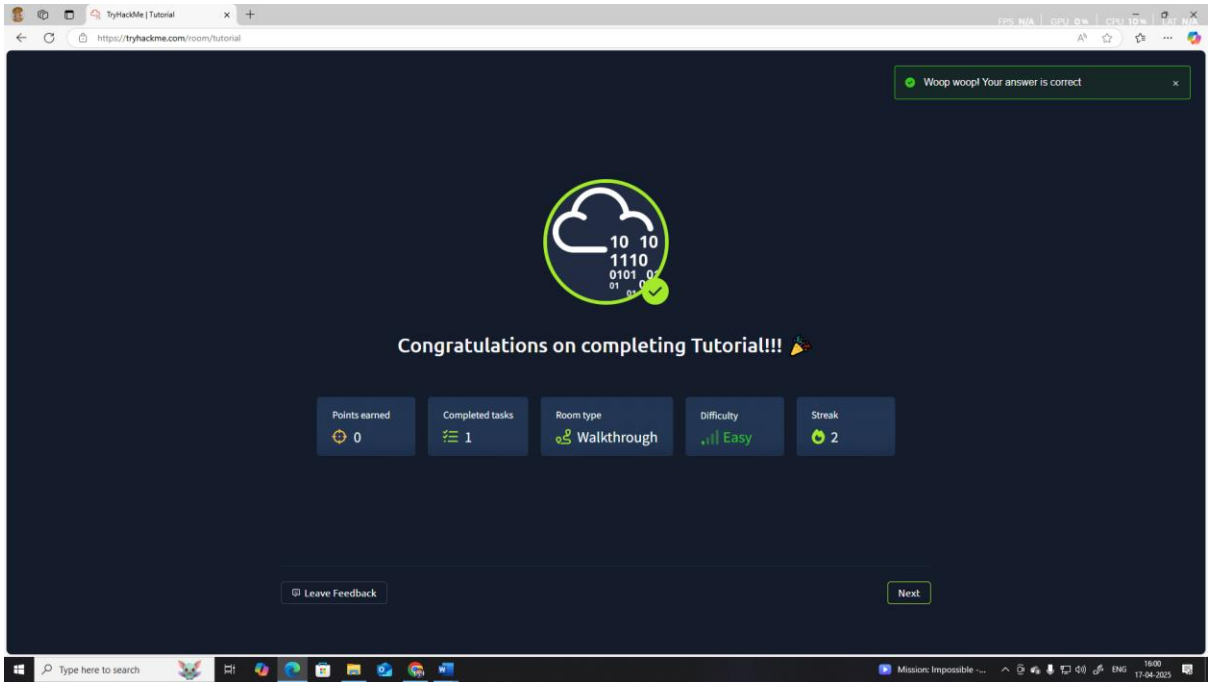
TrackHackMe Room :- TryHackMe Tutorial

1. **Link:-**TryHackMe | Tutorial
2. **Learning Objective:-** Learn the basic structure and navigation of the TryHackMe platform, including how to interact with rooms, answer questions, use hints, deploy virtual machines, and utilize the in-browser AttackBox or your own machine.
3. **Key Tools/Commands Used:-**
   - TryHackMe Web Interface
   - AttackBox (optional)
   - No terminal commands required
   - Platform features like:
     - Join Room
     - Deploy Machine
     - Hints & Answer Boxes
     - Sidebar Navigation

4. **Concepts learned:-**
   - How to join and interact with TryHackMe rooms
   - The structure of rooms: Tasks → Questions → Flags
   - Use of the **Deploy** button and virtual machine interface
   - Introduction to **Answer format** (e.g., THM{} or direct answers)
   - Navigating the TryHackMe UI (Tasks, Progress, Completion)
   - The difference between using **AttackBox** vs. a **local VM**

5. **Walkthrough / How You Solved It:-**
   - **Joined the Room:** Clicked the "Join Room" button to begin.
   - **Followed Step-by-Step Instructions:** Read each task carefully — it explained different parts of the platform.
   - **Deployed the Machine:** Launched the sample virtual machine as guided in the room.
   - **Answered Guided Questions:** These were simple and based on the room's instructions (e.g., identifying what buttons do or what the room structure looks like).
   - **Explored the Interface:** Clicked through available features like the sidebar, hints, and completion progress.
   - **Completed All Tasks:** Submitted all answers correctly by following instructions and checking the UI where needed.

6. **Reflections or Notes:-**
   - This room is extremely beginner-friendly — meant for first-time users of the platform.
   - Helps users understand how TryHackMe works before diving into actual hacking content.
   - No need to worry about tools or commands — it's purely platform familiarization.
   - Quick and easy to complete, but very helpful in setting the foundation.
   - Great refresher even if you've used the platform before but need a walkthrough of updates or layout changes.



TrackHackMe Room :-OpenVPN Configuration

1. **Link:-** TryHackMe | OpenVPN
2. **Learning Objective:-** Understand how to configure and use OpenVPN to securely connect your local machine to TryHackMe's network, allowing interaction with rooms and target machines using your personal setup rather than the AttackBox.

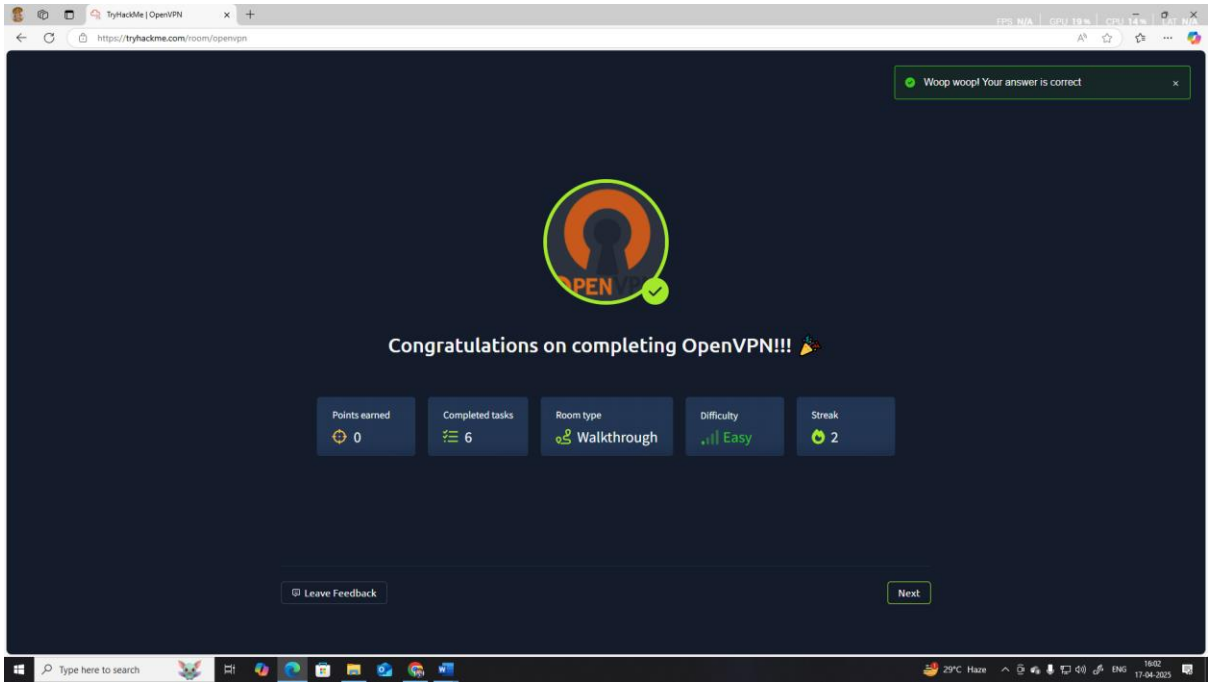
3. **Key Tools/Commands Used:-**
- **OpenVPN** (installed locally)
- **Terminal / Command Prompt**
- **VPN Configuration File (.ovpn)**
- Commands:
    - sudo openvpn <your-config-file>.ovpn
    - ifconfig / ip a (to verify connection)
- Download tools:
    - wget / browser for config file

4. **Concepts learned:-**
- How VPNs work in the context of TryHackMe
- Secure tunneling and private networking basics
- How to download and use your personal .ovpn configuration file
- The difference between using OpenVPN locally vs. the AttackBox
- How to verify a successful VPN connection
- Benefits of using your own virtual machine or Kali OS

5. **Walkthrough / How You Solved It:-**
- Joined the Room

- Downloaded the VPN Configuration File
- Installed OpenVPN
- Ran OpenVPN
- Verified the Connection
- Tested the VPN
- Answered All Questions

7. **Reflections or Notes:-**
   - Essential for users who want a more powerful and customizable hacking setup using their own Kali VM or OS.
   - A VPN connection is more stable and opens up broader tool access than the AttackBox.
   - Important to terminate VPN properly when done: Ctrl+C in terminal.
   - If connection fails, double-check the VPN server region, config file, and whether you're running as root/admin.
   - This room lays the groundwork for transitioning into real-world pentesting lab environments.



TrackHackMe Room :- Beginner Path Introduction

1. **Link:-** TryHackMe | Learning Cyber Security
2. **Learning Objective:-** Provide a foundational understanding of TryHackMe's Beginner Path, introducing users to key concepts and rooms within the path. It aims to prepare users for tackling more technical rooms by explaining the basics of cybersecurity and platform navigation**.**
3. **Key Tools/Commands Used:-**
   - TryHackMe Web Interface
   - In-browser AttackBox (optional for interaction)
   - Virtual Machine Deployment

- Task & Question Boxes
- Hints and Tips Panel

4. Concepts learned:-

- Overview of Beginner Path and how it works on TryHackMe
- Importance of completing rooms in sequence for a structured learning experience
- Basic cybersecurity concepts introduced, such as networking and operating systems
- Understanding the room/task/question flow (including completion tracking)
- Navigation and familiarity with TryHackMe's platform interface
- The concept of learning paths for progressive education in cybersecurity

5. Walkthrough / How You Solved It:-.

- Joined the Room
- Read Room Overview
- Navigated Through the Interface
- Completed Introductory Tasks
- Completed All Tasks.

6. Reflections or Notes:-

- This room is a **great primer** for absolute beginners on TryHackMe, providing insight into how the platform operates and introduces the **Beginner Path** effectively.
- It's not a technical room but sets the stage for future, more hands-on cybersecurity learning.
- It's helpful for familiarizing yourself with the **structure of TryHackMe rooms** and learning what to expect.
- The **Beginner Path** is an excellent starting point for anyone looking to build up knowledge in cybersecurity without feeling overwhelmed by complex tasks.
- I recommend going through this if you're uncertain about where to start your journey on TryHackMe.

TrackHackMe Room :- Starting Out In Cyber Sec

1. **Link:-** TryHackMe | Starting Out In Cyber Sec

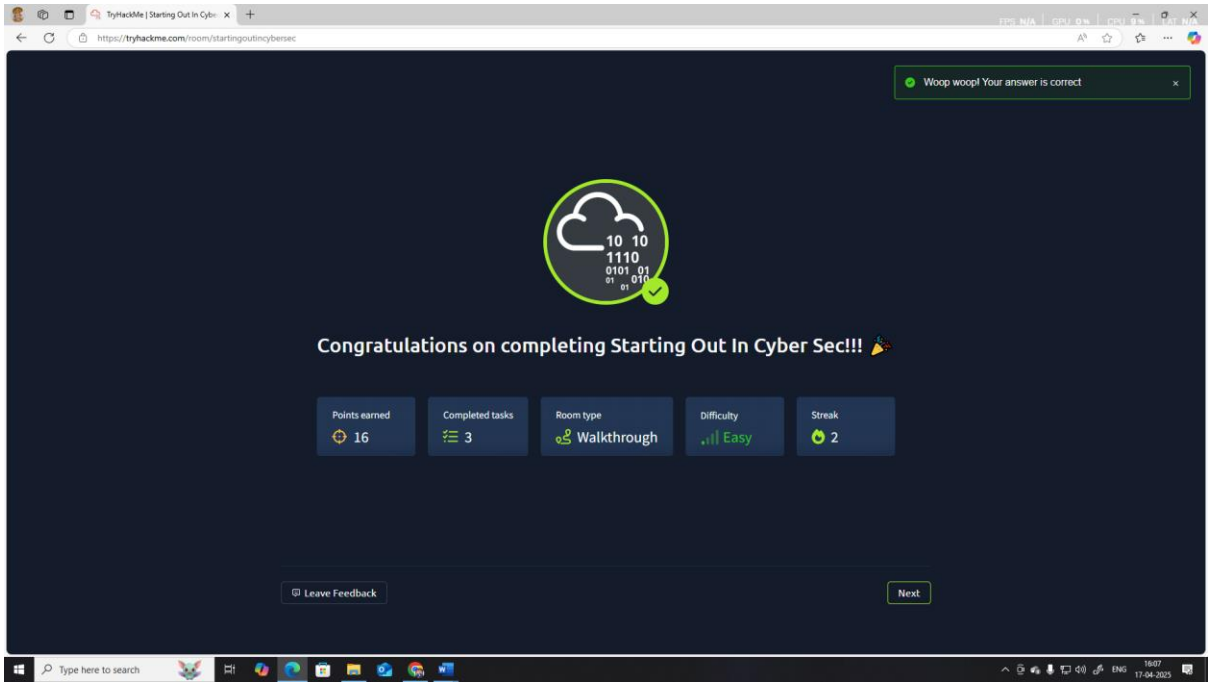
2. **Learning Objective:-** Provide an introduction to the basics of cybersecurity for beginners. This room covers foundational topics, including the importance of cybersecurity, common attack vectors, and basic security principles. It's an excellent starting point for those new to the field.

3. **Key Tools/Commands Used:-**
   - TryHackMe Web Interface
   - In-browser AttackBox (for interaction)
   - Basic Linux commands (such as ls, cat, pwd)
   - Basic networking concepts (e.g., understanding IP addresses, ports)

4. **Concepts learned:-**
   - Introduction to cybersecurity terminology and concepts
   - Overview of common security threats and attack vectors (phishing, malware, etc.)
   - Understanding of basic networking and how it relates to security (IP addresses, ports, firewalls)
   - Importance of secure passwords, encryption, and other security practices
   - Introduction to ethical hacking and basic network reconnaissance techniques.

5. **Walkthrough / How You Solved It:-**.
   - Joined the Room
   - Read Through the Introduction
   - Completed the Tasks
   - Explored the Platform
   - Answered Questions
   - Completed All Tasks

6. **Reflections or Notes:-**
   - A perfect starting point for anyone looking to get into cybersecurity, as it covers basic, essential concepts.
   - This room lays the foundation for deeper cybersecurity topics like ethical hacking, penetration testing, or network security.
   - The room does not involve advanced technical tasks but focuses more on theory and concepts, which is great for beginners.
   - The room's structure is easy to follow, with clear explanations of concepts like phishing and malware, and simple tasks that do not require deep technical expertise.
   - After completing this room, users should feel confident in understanding basic cybersecurity principles and be ready to move on to more technical and hands-on topics like Linux fundamentals, network security, or ethical hacking.



TrackHackMe Room :- Introduction to Research

1. **Link:-**[TryHackMe | Introductory Researching]

2. **Learning Objective:-**Introduce the concept of research in the context of cybersecurity. The room focuses on teaching how to gather information using online resources, tools, and databases. It helps users develop the skill of OSINT (Open Source Intelligence) and using research effectively during penetration testing or cybersecurity investigations.

3. **Key Tool/Command Used:-**
   - Google Search (for gathering information)

4. **Concept Learned:**
   - Effective Searching
   - Credible Sources
   - Utilizing Databases
   - Research Methodologies

5. **Walkthrough / How You Solved It:-**
   - Accesing the room
   - Understanding Search Techniques
   - Exploring Databases:
   - Task Completion
   - Evaluating Sources

6. **Reflections or Notes:-**
   - This room is crucial for developing essential research skills needed for any cybersecurity professional.

- It highlights the importance of effective searching, evaluating sources, and utilizing databases to gather reliable information.
- Mastering these skills is fundamental for staying informed about emerging threats, vulnerabilities, and security best practices.